UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/033,102	10/25/2001	Robert D. Gardner	10011537-1	7724

7590 12/29/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
ALI, SYED J

ART UNIT	PAPER NUMBER
2195	

DATE MAILED: 12/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/033,102	**Applicant(s)** GARDNER, ROBERT D.	
	Examiner Syed J. Ali	**Art Unit** 2195	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *Oct. 11, 2005*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the amendment filed October 11, 2005. Claims 1-26 are presented for examination.

2. The text of those sections of Title 35, U.S. code not included in this office action can be found in a prior office action.

Claim Rejections - 35 USC § 102

3. **Claims 1-2, 11, and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by McNabb et al. (USPN 6,289,462) (hereinafter McNabb).**

4. As per claim 1, McNabb teaches the invention as claimed, including a computer system comprising:

at least one processor (col. 6 lines 28-29);

a memory (col. 1 lines 11-18; Fig. 1);

a secure platform stored in the memory for controlling the processor and the memory (col. 7 lines 11-20);

an operating system image stored in the memory for controlling the processor and the memory and operating on top of the secure platform (col. 8 line 54 - col. 9 line 10);

an end user application stored in the memory for controlling the processor and the memory and operating on top of the operating system image (col. 9 lines 34-36); and wherein the secure platform is configured to provide a secure partition within the memory for storing secret data associated with and accessible by the end user application (col. 4 lines 20-24), the secure partition being inaccessible to the operating system and other tasks operating on top of the secure platform (col. 17 lines 7-17, 52-61).

5. As per claim 2, McNabb teaches the invention as claimed, including the computer system of claim 1, wherein the at least one processor has at least three execution privilege levels including a first privilege level, a second privilege level that is less privileged than the first privilege level, and a third privilege level that is less privileged than the second privilege level· (col. 12 lines 50-65).

6. As per claim 11, McNabb teaches the invention as claimed, including the computer system of claim 1, wherein the end user application includes a secure process indicator for indicating that the end user application is to be treated as a secure process (col. 10 lines 10-25).

7. As per claim 26, McNabb teaches the invention as claimed, including a computer readable medium containing the components of the computer system of claim 1 (Fig. 1).

Claim Rejections - 35 USC § 103

8. **Claims 3-6 and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over McNabb.**

9. As per claim 3, McNabb teaches the invention as claimed, including the computer system of claim 2, wherein the end user application is configured to operate at the third privilege level as an unprivileged task (col. 9 lines 57-67), the operating system image is configured to operate at the second privilege level as an unprivileged task (col. 12 line 61 - col. 13 line 6), and at least a first portion of the secure platform is configured to operated at the first privilege level as a privileged task (col. 10 lines 60-65; col. 11 lines 3-9).

10. It is noted that McNabb does not necessarily limit the privilege levels of the end user application, as certain applications may be granted superuser status. However, the default level for the end user application is the "least" privilege level, such that it is ensured that it is properly authenticated before giving it access to the relevant partition. The secure platform operates at a highest privilege level, as it is the module that implements security and controls access to the processor and memory. Secondly, the operating system operates at a level between the secure platform and the end user application, and inherently has a privilege level that is less than the secure platform, but greater than the end user application. The operating system resides on top of the secure platform and acts as a negotiator to allow the end user application access to secret data. Finally, the end user application has a level of privileges assigned to it, depending on the partitions that it needs to access. These privileges may be increased or decreased depending on the sections of memory that it must access.

11. As per claim 4, McNabb teaches the invention as claimed, including the computer system of claim 3, wherein the first portion of the secure platform is a secure platform kernel (SPK) (col. 10 lines 60-65; col. 11 lines 3-9).

12. As per claim 5, McNabb teaches the invention as claimed, including the computer system of claim 4, wherein the SPK performs security critical services including memory services (col. 7 lines 11-20).

13. As per claim 6, McNabb teaches the invention as claimed, including the computer system of claim 5, wherein the security critical services performed by the SPK further include process services, cryptographic services, and exception handling (col. 7 lines 11-20).

14. As per claims 18-21, McNabb teaches the invention as claimed, including a computer system according to claims 1-6 (Fig. 1).

15. **Claims 7-10, 12-17, and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over McNabb in view of Quach et al. (USPN 6,654,909) (hereinafter Quach).**

16. As per claim 7, Quach teaches the invention as claimed, including the computer system of claim 1, wherein the at least one processor includes:

protection key registers configured to hold protection keys (col. 2 lines 65-67), which the secure platform employs to control access to security critical structures (col. 2 lines 38-39).

17. It would have been obvious to one of ordinary skill in the art to combine McNabb and Quach since the use of protection keys allows data associated with critical resources to be consumed without being taken out of memory. Thus, resources that are used more than once do not have to be re-authenticated each time that an application accesses the resource. This is much more efficient than performing a potentially computationally intensive authentication procedure each time that an application accesses a resource.

18. As per claim 8, Quach teaches the invention as claimed, including the computer system of claim 7, wherein the security critical structures include the secure partition (col. 1 lines 35-43).

19. As per claim 9, McNabb teaches the invention as claimed, including the computer system of claim 8, wherein the secure partition includes at least one memory page (col. 7 lines 44-47).

20. As per claim 10, McNabb teaches the invention as claimed, including the computer system of claim 7, wherein the security critical structures include the end user application (col. 17 lines 52-61).

21. As per claim 12, McNabb teaches the invention as claimed, including a method of controlling the computer system of claims 1-4 and 7 (col. 1 lines 11-18; Fig. 1).

22. As per claim 13, Quach teaches the invention as claimed, including the method of claim 12, and further comprising:

monitoring execution of instructions of the end user application (col. 2 line 52 - col. 3 line 27); and

flushing the first protection key value from the protection key registers when execution of the end user application instructions stops (col. 1 lines 37-43).

23. As per claim 14, Quach teaches the invention as claimed, including the method of claim 13, and further comprising:

reinserting the first protection key value in one of the protection key registers when execution of the end user application instructions resumes (col. 1 lines 45-46).

24. As per claim 15, McNabb teaches the invention as claimed, including the method of claim 12, wherein the allocating a portion of the memory is performed by the SPK (col. 10 lines 60-65; col. 11 lines 3-9).

25. As per claim 16, Quach teaches the invention as claimed, including the method of claim 12, wherein the first protection key value is inserted in one of the protection key registers by the SPK (col. 2 line 52 - col. 3 line 27).

26. As per claim 17, Quach teaches the invention as claimed, including the method of claim 12, and further comprising:

associating a second protection key with the end user application to prevent unauthorized modifications (col. 2 line 52 - col. 3 line 27).

27. As per claims 22-25, McNabb teaches the invention as claimed, including a computer system according to claims 7-10 (col. 1 lines 11-18; Fig. 1).

Response to Arguments

28. **Applicant's arguments filed October 11, 2005 have been fully considered but they are not persuasive.**

29. In numerous places Applicant asserts that McNabb is "*unrelated to the current application*" or "*unsuitable to* [sic] *an anticipatory reference*." Applicant argues that the claimed invention is a "*new computer architecture*" and that McNabb improves "*a currently available operating system*" and thus does not teach or suggest a "*new computer architecture*."

30. With respect to the above arguments, Examiner submits that they are entirely inappropriate as traversal arguments. The claim is directed to the features of the "new computer architecture", not the mere fact that the architecture is "new". These features include a "secure platform" that is capable of providing secure partitions that allow access to data by applications that are not accessible to the operating system. Thus, if a prior art references teaches these features, it is anticipatory, regardless of whether it is a "new computer architecture" or "unrelated to the ... application." *See State Contracting & Eng ' g Corp. v. Condotte America, Inc.*, 346 F.3d 1057, 1068 (Fed. Cir. 2003) ("The question of whether a reference is analogous art is not

relevant to whether that reference anticipates. A reference may be directed to an entirely different problem than the one addressed by the inventor, or may be from an entirely different field of endeavor than that of the claimed invention, yet the reference is still anticipatory if it explicitly or inherently discloses every limitation recited in the claims").

31. Applicant argues that McNabb does not anticipate the claimed invention because there is no teaching or suggestion of a "*secure platform*" that provides "*a secure partition accessible to an end-user application but not to an operating system.*"

32. First, it appears to Examiner that Applicant has mischaracterized McNabb and overlooked the features relating to the "secure platform." The "secure platform" is not the disclosed operating system enhancements, as Applicant suggests throughout the arguments, but the security features that are coupled to the operating system enhancements to make the entire system more secure. Applicant includes an operating system <u>and</u> a secure platform within the computer architecture, but by no means is the operating system understood to be the same thing as the secure platform. In like fashion, McNabb includes an operating system as part of the architecture; there would be no control over the computer without an operating system. The mere fact that McNabb teaches operating system enhancements to improve its security does not mean that the rest of the reference should not be considered. In addition to the operating system enhancements, McNabb provides Advanced Secure Networking ("a security component...to indicate which compartment or partition [a] packet belongs to"), an Upgrade/Downgrade enforcer ("a component...to examine each incoming request and decide which application...should handle it"), and a Security Gate ("a software component that allows limited,

secure communication between applications or utilities operating in separate partitions"). These features collectively act as a secure platform that regulates various system activities to ensure that each is acting within its delegated permissions, i.e. within its 'sensitivity level'. The communication is organized in such a way that packets, requests, and applications are regulated to pass through their respective secure software components, bypassing the operating system (col. 17 lines 7-15, "data in a back-end application resides in its own compartment...ensuring that the back-end application will be accessible only through the security gate").

Conclusion

33. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed J. Ali whose telephone number is (571) 272-3769. The examiner can normally be reached on Mon-Fri 8-5:30, 2nd Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai T. An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Syed Ali
May 24, 2005

MENG-AL T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100